IN THE CLAIMS:

1. (Previously presented) A method for authenticating a message, comprising:

performing a security function upon the message to generate a message authentication code, wherein the security function utilizes at least one publicly known constant to perform the security function upon the message, and wherein the at least one publicly known constant is selected from a set of publicly known constants used to implement the security function;

sending the message to a receiver;

sending the message authentication code to the receiver; and

sending the at least one publicly known constant, used by the security function to perform the security function upon the message, to the receiver, wherein the receiver authenticates the message based on the message authentication code and the at least one publicly known constant.

2. (Original) The method of Claim 1, wherein the security function comprises a hash function.

3. (Previously presented) The method of Claim 1, wherein the authentication comprises a determination that the message is at least one of authentic or not authentic.

4. (Canceled)

5. (Previously presented) The method of Claim 1, wherein the security function further comprises at least one of an encryption function or a decryption function.

6-16. (Canceled)

17. (Previously presented) The method of Claim 1, wherein the security function is a Secure Hash Algorithm (SHA), and wherein the set of publicly known constants comprises the first 64 bits of the fractional parts of the cube roots of the first eighty prime numbers.

18. (Previously presented) The method of Claim 1, wherein the receiver does not store the set of publicly known constants.

19. (Previously presented) The method of Claim 1, further comprising:

authenticating, at the receiver, the message as a function of at least a shared key, the at least one publicly known constant, the security function, the message, and the message authentication code.

20. (Canceled)

21. (Previously presented) The method of Claim 2, wherein the hash function is applied to a secret key, the at least one publicly known constant, and the message such that the resulting message authentication code is equal to a hash of the combination of the secret key, the at least one publicly known constant, and the message.

22-25. (Canceled)